UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

TAMARA WILSON, *individually and on behalf of all others similarly situated*, Plaintiff, v. TRILLER, INC., a Delaware corporation, Defendant.	Case No.: 21-cv-11228

MEMORANDUM IN OPPOSITION TO DEFENDANT TRILLER, INC.'S MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Rules and Statutes

Other Authorities

INTRODUCTION

Plaintiff Tamara Wilson brought this class action against Defendant Triller after discovering that Triller collected and shared personal information about her video watch history with third parties without her consent. One of Triller's primary arguments for why Plaintiff's case should be dismissed—that "all of the allegedly shared information is anonymous and not traceable to Plaintiff"—is becoming recognized as a "flawed, dangerous narrative." *See* Justin Sherman, *Big Data May Not Know Your Name. But it Knows Everything Else*, Wired (Dec. 19, 2021).[1]

> [Y]ou can basically reidentify anything. "Anonymity" is an abstraction. Even if a company doesn't have your name (which they probably do), they can still acquire your address, internet search history, smartphone GPS logs, and other data to pin you down. . . . Reidentification has become horrifyingly easy. In 2006, when AOL published a collection of 650,000 users' 20 million web searches, with names replaced by random numbers, *The New York Times* very quickly linked the searches to specific people. ("It did not take much," the reporters wrote.) Two years later, researchers at UT Austin famously matched 500,000 Netflix users' "anonymized" movie ratings against IMDb and identified the users as well as "their apparent political preferences and other potentially sensitive information." . . .
>
> The irony that data brokers claim that their "anonymized" data is risk-free is absurd: Their entire business model and marketing pitch rests on the premise that they can intimately and highly selectively track, understand, and microtarget individual people.
>
> This argument isn't just flawed; it's also a distraction. Not only do these companies usually know your name anyway, but data simply does not need to have a name or social security number attached to cause harm.

[1] As cited in Plaintiff's Complaint (ECF No. 1, "Compl.") ¶ 66, n.9.

Id.[2] While Triller argues that its actions in connection with Plaintiff's use of its "free" app have not amounted to any cognizable violation of the statutory and common law claims alleged in Plaintiff's Complaint (or, alternatively, that Plaintiff disclaimed any liability or consented to Triller's actions by terms she never agreed to), the reality is that Triller's amassing and sharing of this type of data without adequate disclosure or consent is a violation of state and federal law.

ARGUMENT

A complaint "does not need detailed factual allegations" to survive a motion to dismiss under Rule 12(b)(6) of the Federal Rules of Civil Procedure. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A complaint need only include "enough facts to state a claim to relief that is plausible on its face." *Id*. at 570. A claim has facial plausibility and is sufficient to survive a motion to dismiss when the plaintiff pleads factual content that allows the Court, based on its experience and common sense, to draw the reasonable inference that the defendant is liable for the misconduct alleged. *Id*. at 556. Rule 8(a)(2) of the Federal Rules of Civil Procedure does not require specific facts; the statement need only "give the defendant fair notice of what the. . . claim is and the grounds upon which it rests." *Twombly*, 550 U.S. at 555. The plausibility standard is *not* akin to a "probability requirement," but asks for more than a sheer possibility that a defendant has acted unlawfully. *Id*. at 556; *Palmer v. Fannie Mae*, 755 Fed. Appx. 43, 45 (2d Cir. 2018).

The Court must accept as true all of Plaintiffs' allegations of material fact and construe them in the light most favorable to the Plaintiff. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678-80 (2009).

[2] *See also* Daniel L. Macioce, Jr., *Pii in Context: Video Privacy and A Factor-Based Test for Assessing Personal Information*, 45 Pepp. L. Rev. 331, 348–49 (2018) ("[S]earch by search, click by click, the identity of AOL user No. 4417749 became easier to discern. . . . It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments[,] and loves her three dogs.")

To the extent the Court finds defects in the pleadings sufficient to warrant dismissal, that dismissal should be without prejudice to permit Plaintiff to repair the defect. Fed. R. Civ. P. 15(a); *e.g., Palm Beach Mar. Museum, Inc. v. Hapoalim Sec. USA, Inc.*, 810 F. Appx 17, 18 (2d Cir. 2020) (remanding case to district court to consider whether leave to amend appropriate); *Palmer*, 755 Fed. Appx. at 45 (finding error in not allowing plaintiff to amend complaint after trial court dismissed claims with prejudice). Plaintiff requests leave to amend if any portion of her complaint is deficient

I. Triller's use of dark patterns prevents users from understanding and agreeing to material terms.

As an initial matter, Plaintiff alleges that Triller "makes no effort to ensure that users see the full text of its Terms of Use and Privacy Policy" because "there is no requirement that the user agree to any of the privacy provisions set out in the Privacy Policy" when downloading the Triller app. Compl. ¶ 70. There is no requirement that the app user read or accept Triller's Privacy Policy before using the app, nor is there a pop-up notification regarding Triller's Privacy Policy (or that it even has a privacy policy). *Id.* ¶¶ 72-73. Only when attempting to "log in" or "sign up" is the app user finally brought to a page that makes reference to "Terms of Service" and a "Privacy Policy" placed at the very bottom of the page in much smaller type than any other links on the page. *Id.* ¶ 74-75. Triller's decisions on how to display its Terms are intentional—to ensure that users do not read either the Terms of Service or the Privacy Policy. *Id.* at 78-80. In fact, users can download the app and begin watching videos without reading or agreeing to any of Triller's terms. *Id.* ¶¶ 77-78. M. Darren Traub, Triller's General Counsel, does not even attempt to dispute any of these allegations in his declaration in support of Triller's motion to dismiss. *See* ECF No. 35.

Ignoring that Plaintiff alleged that Triller purposely hides its Terms of Service and Privacy Policy (collectively, "Terms"), Triller argues Plaintiff provided consent to the disclosure of her

personally identifiable information ("PII") to third parties and that she agreed to limit Triller's liability. *See* Triller Mot. at 12-16, 21-23. But Triller is wrong. Plaintiff's claims are not barred by its Terms because "there is a 'bona fide dispute as to the existence of a contract, [and whether it] cover[s] the dispute in issue[.]'"*Poller v. BioScrip, Inc.,* 974 F. Supp. 2d 204, 236 (S.D.N.Y. 2013) (citation omitted).[3]

In *Scotti v. Tough Mudder Inc.,* the New York Supreme Court explained that "[t]he creation of online contracts 'has not fundamentally changed the principles of contract.'" 63 Misc. 3d 843, 846, 97 N.Y.S.3d 825, 831 (N.Y. Sup. Ct. 2019) (citing *Resorb Networks, Inc. v. YouNow.com*, 51 Misc. 3d 975, 981, 30 N.Y.S.3d 506 (Sup. Ct. N.Y. County 2016), quoting *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 403 (2d Cir. 2004)). Thus, the court held that "[t]the question of whether there is agreement to accept the terms of an on-line contract turns on the particular facts and circumstances. Courts generally look for evidence that a website user had actual or constructive notice of the terms by using the website." *Id*.

In *Berkson v. Gogo LLC*, 97 F. Supp. 3d 359 (E.D.N.Y. 2015), this District's sister court set out three, general principles regarding validity and enforceability of internet contracts. First, online "terms of use" will be enforced only when the website puts a reasonably prudent user on inquiry notice of those terms. *Id.* at 401 (citing *Nguyen v. Barnes & Noble Inc*., 763 F.3d 1171,1177 (9th Cir. 2014)*).* Second, online "terms of use" will be enforced when a user is encouraged by the design and content of the website to examine the terms clearly available via hyperlink. *Id*. Third,

[3] Triller's reliance on *Himmelstein v. Matthew Bender & Co. Inc.* is inapt, because unlike that case, Plaintiff does not bring a claim for breach of contract. No. 650932/2017, 2018 WL 984850, at *6 (N.Y. Sup. Ct. N.Y. Cnty. Feb. 6, 2018). Also unlike *Koenig v. Boulder Brands, Inc.*, Plaintiff's unjust enrichment claim is not based on Defendant's "purported misrepresentations." 995 F. Supp. 2d 274, 290-91 (S.D.N.Y. 2014).

online "terms of use" will not be enforced where the link to the terms is "buried at the bottom of a webpage or tucked away in obscure corners of the website where users are unlikely to see it." *Id*. at 401-402.

The *Berkson* court outlined a four-part inquiry for assessing the validity and enforceability of electronic adhesion contracts specifically. *Id*. at 402. First, aside from signing in, is there substantial evidence from the website that the user was aware of the terms to which they were binding themselves? *Id*. Second, do the design and contents of the website make the terms readily and obviously available to the user? *Id*. Third, is the importance of the details clearly visible, and not obscured or minimized? *Id*. Fourth, does the vendor clearly draw the consumer's attention to material terms that would alter what a reasonable consumer understands to be their default rights in such a transaction? *Id.* Only answers in the affirmative make the electronic adhesion contract enforceable, and the vendor bears the burden of showing a party's agreement to the contract. *Id.* at 402-403.

Numerous other cases have held that contractual provisions in online terms of service such as Triller's are unenforceable when the contract is not reasonably conspicuous, and thus there is no unambiguous manifestation of assent by plaintiff. In *Scotti*, the defendant contended plaintiffs agreed to a mandatory arbitration clause when registering for the defendant's event online and clicking a box next to a statement that read: "I agree to the above waiver." *Id*. at 829. The court ultimately held the defendant failed to establish its webpage provided reasonable notice of the relevant provision, rendering it unenforceable. *Id*. at 834. The court reasoned:

> A party may be bound to a click wrap agreement by clicking a button declaring assent, so long as the party is given a "sufficient opportunity to read the ... agreement, and assents thereto after being provided with an unambiguous method of accepting or declining the offer…" … "[a] court cannot presume that a person who clicks on a box that appears on a ... screen has notice of all contents not only of

> that page but of other content that requires further action (scrolling, following a link, etc.)"

Id. at 832 (citing *Serrano v. Cablevision Sys. Corp.*, 863 F. Supp. 2d 157, 164 (E.D.N.Y. 2012), *Applebaum v. Lyft, Inc*., 263 F.Supp.3d 454, 466 (S.D.N.Y. 2017)). *See also Edme v. Internet Brands, Inc*., 968 F. Supp. 2d 519, 526 (E.D.N.Y. 2013) (denying defendant's motion to dismiss because the court could not ascertain the circumstances surrounding how defendant's website's Terms of Use appeared to its users, which was determinative as to whether the plaintiff had actual or constructive notice of the terms and conditions, including whether the disputed forum selection clause was reasonably communicated).

Because Triller did not provide "clear and conspicuous" notice of its Terms, Plaintiff is not bound by them. *See Starke v. SquareTrade, Inc*., 913 F.3d 279, 289 (2d Cir. 2019) (holding that plaintiff was not on sufficient notice of the terms and conditions not clearly disclosed); *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 235 (2d Cir. 2016) (applying Washington law, finding inconspicuous notice of Amazon's terms on a cluttered order page); *cf. Meyer v. Uber Techs.*, Inc., 868 F.3d 66, 78 (2d Cir. 2017) (finding defendant provided conspicuous notice on uncluttered signup screen). In considering whether the notice is conspicuous, courts analyze the "totality of the circumstances," including "the design and content of the relevant interface to determine if the contract terms were presented to the offeree in a way that would put [the offeree] on inquiry notice of such terms." *Starke*, 913 F.3d at 297. As alleged, Triller obscures the Terms during signup, by: (1) disclosing the existence of these terms in "the smallest text" on the signup page, (2) positioning the disclosure "at the bottom of the page, below all of the other brightly colored login or sign-up buttons," and (3) not presenting the Terms as a mandatory step, and not requiring

acknowledgement from the user that they have read and understood these Terms. Compl. ¶ 76.[4] While Triller's General Counsel provides the Court with the written Terms, themselves, he fails to dispute—at all—Plaintiff's allegations that they were hidden, and not presented at the time that users downloaded and used the app. Taking these circumstances together, there is no way a reasonable user would have understood that by signing up for an account, they agreed to be bound by Triller's misleading Terms. And for users who have not signed up for an account, but nonetheless use Triller to view videos, there is no reasonable basis to conclude they even knew of, much less assented to, Triller's Terms. *Id.* ¶ 77.

Concerning Plaintiff's unjust enrichment claim, the Terms do not disclose the alleged misbehavior, including the information that was collected by Triller, and the information that was disclosed by Triller.[5] *See Premier Medical Systems, LLC v. Neurological Corp.*, No. 1:21-CV-1337-GHW, 2022 WL 603999, at *8 (S.D.N.Y. Feb. 28, 2022) (upholding a claim for unjust enrichment where the parties disagreed about the scope of the agreement); *Union Bank, N.A. v. CBS Corp.*, 2009 WL 1675087, at *8 (S.D.N.Y. June 10, 2009) (declining to dismiss unjust

[4] Indeed, Plaintiff says that she does not recall seeing the Terms of Service or Privacy Policy upon registering for an account with the app. Compl. ¶ 7. Triller argues that "Plaintiff's allegations show that she consented to the Terms by signing up for an account," Triller Mot. at 12, and that "Plaintiff alleges that. . . the notice of disclosure in Triller's Terms was given to all users who sign up," *Id.* at 13, but that is not the case and wholly disputed by the allegations in Plaintiffs' Complaint.

[5] Plaintiff's unjust enrichment claim is also not duplicative of the statutory claims because the statutory claims require additional proof not required in a claim for unjust enrichment. *See Warner v. StarKist Co.*, No. 118CV406GLSATB, 2019 WL 1332573, at *3 (N.D.N.Y. Mar. 25, 2019) (denying motion to dismiss unjust enrichment claim where it was distinct from the elements of plaintiffs' statuary claims); *McCracken v. Verisma Sys.*, Inc., No. 14-CV-06248(MAT), 2017 WL 2080279, at *8 (W.D.N.Y. May 15, 2017) (same). Whereas the VPPA, CFFA, and ICFA each require specific levels of proof regarding the type of information collected and disclosed; a claim for unjust enrichment only requires a showing of the following: "(1) that the defendant benefitted; (2) at the plaintiff's expense; and (3) that equity and good conscience require restitution." *Beth Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of N.J., Inc.*, 448 F.3d 573, 586 (2d Cir. 2006).

enrichment claim where resolving the dispute may require "going outside the four corners of the parties' agreements"). Plaintiff may seek compensation for Triller's use of Plaintiff's information that are not addressed by the Terms, such as the substantial revenues from the disclosure of Plaintiff's PII to third parties. *Id.* ¶ 123.

Defendant bears the burden to demonstrate Plaintiff agreed to the Terms—especially when arguing that those Terms limit its liability, or prevent a plaintiff from bringing a particular claim. But Triller has failed to do so, here. This failure is fatal to Triller, especially on a motion to dismiss when all disputed facts are weighed in Plaintiff's favor.

II. Triller shares personally identifiable information, in violation of the Video Privacy Protection Act, without user consent.

A. Triller shares Plaintiff's and class members' PII with third parties.

Triller does not dispute that it shared Plaintiff's video watching history with third parties; it instead argues primarily that a district court case and an out-of-circuit appellate court case dictate that, so long as Triller did not share Plaintiff's "name, actual date of birth, or personal address," her claim should be dismissed. Triller Mot. at 11. But Triller's analysis of these prior cases ignores that newer technology—indeed, the technology that Triller uses—*can* and *does* disclose the identities of individuals to third parties like Facebook and Appsflyer. Moreover, through its limiting definition of PII, Triller ignores that courts and Congress, alike, routinely recognize that other identifiers can constitute PII—like Social Security numbers and GPS coordinates.

Plaintiff alleges that Triller assigns a unique identifier (or "UID") to each Triller user, and that UID is only associated with one user account, persistent across devices. Compl. ¶¶ 39-40. That UID is associated with a unique "advertiser_id," which is transmitted to Facebook and Appsflyer, "along with other personal information while a user is logged on to the platform." Compl. ¶¶ 41-42. What Triller shares with Facebook and Appsflyer does not end there:

> When a user visits her profile page, Triller pairs the UID and handle with other data from the user's profile page including (but not limited to) anything written in the "About Me" section, the URL of the photo chosen by the user for as an avatar (a photographic representation of the user) on the app, whether or not the user has a linked Instagram account (and, if so, the linked Instagram handle), whether or not the user has listed a Soundcloud URL or linked Snapchat account, and any photos or videos viewed and/or liked by the user on her profile.
>
> By pairing this information with the UID, Facebook and Appsflyer can easily associate UIDs with the individual user.
>
> Further, when a user watches a video, an event indicating the video ID and the creator handle is created and sent to both Facebook and Appsflyer, regardless of whether or not the user watching the video has connected a Facebook (or any other) account to Triller.

Compl. ¶¶ 43-44. That information is then combined with where the user resides, the time zone of the user, and the user's device information. *Id.* ¶ 54. "As a result, Facebook can easily compile a dossier on any given user which aggregates the user's video watch history and associates it with their PII." *Id.* ¶ 60. Moreover, Facebook and Appsflyer "can easily associate" the information Triller shares "with the individual user." *Id.* ¶ 44. That is: Facebook and Appsflyer can determine who the user is by the information Triller shares.

The VPPA's language is "broad," and defines "personally identifiable information" to "*include[] information which identifies* a person as having requested or obtained specific video materials or services from a video tape service provider." *Mollett v. Netflix*, 795 F.3d 1062, 1066 (9th Cir. 2015) (emphasis added); 18 U.S.C. § 2710(a)(3). "As an initial matter, 'personally identifiable information' must include more information than that which, by itself, identifies an individual as having watched certain videos. Instead, 'personally identifiable information' covers some information that *can be used* to identify an individual." *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 984 (9th Cir. 2017) (emphasis original). As the court in *Eichenberger* continued, "the term 'personally identifiable information' covers some information that is 'capable of' identifying

a person, as well as information that, standing alone, identifies a person." *Id.* While all courts recognize that the language of the VPPA is non-exhaustive, and that many types of information constitute PII, there are two recognized approaches to determining whether an entity has shared someone's PII—a narrower approach based upon a hypothetical, "ordinary" recipient adopted by the Third Circuit (which Triller asks this Court to apply), and a fact-specific approach adopted by the First Circuit that is more in line with the purpose of the VPPA.[6]

The First Circuit's standard on "personally identifiable information" encompasses "information *reasonably and foreseeably likely* to reveal which. . . videos [a person] has obtained." *Yershow v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 486 (1st Cir. 2016) (emphasis added). After noting that the definition of PII provided in the VPPA "adds little clarity beyond training [the court's] focus on the question whether the information identifies the person who obtained the video," the court recognized that "PII is not limited to information that explicitly names a person." *Id.* at 486. Like other courts to consider the definition, the First Circuit focused on the use of the word *includes*, which it found to suggest that "the proffered definition falls short of capturing the whole meaning." *Id.* Moreover, the court found support in the VPPA's legislative history that "the drafters' aim was 'to establish a minimum, but not exclusive, definition of personally identifiable information." *Id.*

> Many types of information other than a name can easily identify a person. Revealing a person's social security number to the government, for example, plainly identifies the person. Similarly, when a football referee announces a violation by "No. 12 on the offense," everyone with a game program knows the name of the player who was flagged.

Id. While the information shared by the defendant in *Yershov* with third-party Adobe did not

[6] Triller neither addresses nor distinguishes the First Circuit's approach in its motion.

amount to the plaintiff's "name, actual date of birth, or personal address," the court acknowledged that the defendant reasonably knew that—like with Facebook, here—Adobe could use the information provided by the defendant (such as GPS coordinates) to determine the plaintiff's identity. *Id.*[7]

Triller argues that this Court should follow the Third Circuit's more narrow interpretation of PII, which provides that PII covers only "the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching history." *In re Nickelodeon Consumer Privacy Litig*., 827 F.3d 262, 282 (3d Cir. 2016), *cert. denied sub nom*. *C. A. F. v. Viacom Inc*., 137 S. Ct. 624 (2017).[8] In that case, plaintiffs alleged that the use of internet cookies violated the VPPA, among other things. *Id.* at 268-69. The court determined that "personally identifiable information" was simply "information that would, with little or no extra effort, permit an ordinary recipient to identify a particular person's video-watching habits." *Id.* at 284. The Third Circuit's narrow interpretation of PII was based on the court's doubt that the VPPA could be

[7] A name is only one kind of personally identifiable information, and PII need not be akin to a name. Information can be identifiable when it "describes a relationship between the information and a person, namely that the information—whether sensitive or trivial—is somehow identifiable to an individual." Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1207 (1998). Information can be "identifiable" to a person in one of three ways: (1) authorship (information someone creates), (2) description (providing a person's characteristics like sex and age), or (3) instrumental mapping (unique identifiers like Social Security numbers or MAC or device addresses). *Id*.

[8] Other cases cited by Triller offer important differences to the facts here—namely, that third parties *may* have been able to identify individuals by potentially linking disclosures to information collected from other sources, like in *Robinson v. Disney Online*, 152 F. Supp. 3d 176, 184 (S.D.N.Y. 2015), *Ellis v. Cartoon Network, Inc.*, 2014 WL 5023535 (N.D. Ga. Oct. 8, 2014), *aff'd on other grounds* 803 F.3d 1251 (11th Cir. 2015), and *Eichenberger v. ESPN, Inc.*, 2015 WL 7252985 (W.D. Wash. May 7, 2015). Here, Facebook—as alleged by the Plaintiff—would not need to link it to information collected from other sources; it already has the information, and Triller knows that. *Cf. In re Hulu Priv. Litig.*, 2014 WL 1724344, at *13-14 (N.D. Cal. Apr. 28, 2014) (acknowledging that information disclosed to Facebook, which was sufficient to identify a Facebook user, constituted PII under the VPPA).

applied to "a contemporary understanding of Internet privacy," *id.* at 290; that is, how "anonymized" or "pseudonymized" information could be used to identify an *actual* person.[9]

But this narrow interpretation ignores the very privacy concerns implicated in the VPPA. The Senate Report for the law unequivocally establishes "that the drafters' aim was 'to establish a minimum, but not exclusive, definition of personally identifiable information.'" *Yershov*, 820 F.3d at 486 (quoting S. Rep. No. 100-599, at 12). The Third Circuit recognized that in prohibiting the disclosure of "personally identifiable information" Congress was using "a term of art." *Nickelodeon*, 827 F.3d at 292 n. 186. That "term of art" regularly encompasses types of information used to "distinguish or trace" an individual and which are "linked or linkable" to an individual. *See* Nat'l Inst. of Standards & Tech., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Special Pub. 800-122, at 2-1 (Apr. 2010), http://1.usa.gov/1DgxrRy.[10] Explaining this definition, the NIST notes that whether a set of information was personally identifiable depended on the information a particular recipient—like Facebook, here—could access. *See id.* (discussing a scenario in which "someone with access to both databases may be able to link the information from the two databases and identify individuals"). If courts are to recognize that PII refers to a term of art, then the Court should follow

[9] *But see* Antonin Scalia & Bryan Garner, *Reading Law* 86 (1st ed. 2012) ("broad language [like that of the VPPA] can encompass the onward march of science and technology."). While on the one hand the words of a statute should be given the meaning they carried when the statute was enacted, "[d]rafters of every era," Scalia and Garner explain, "know that technological advances will proceed apace and the rules they create will one day apply to all sorts of circumstances that they could not possibly envision." *Id.*

[10] The NIST, part of the Department of Commerce, is tasked by Congress to develop information security guidelines for all federal agencies. 15 U.S.C. § 278g-3(a)(3).

the standard set out in *Yershov* and allow Plaintiff's claim to proceed.[11]

B. Triller did not provide notice, and Plaintiff did not consent, to Triller sharing her PII.

A video tape service provider may disclose PII concerning any consumer to any person *only with the informed, written consent of the consumer given at the time the disclosure is sought*. 18 U.S.C. § 2710(b)(2)(B) (emphasis added). Given that Plaintiff disputes she even saw the Terms before using the Triller app, *supra* Section I, Triller's argument—that "Plaintiff received written notice and provided consent to Triller to collect and share information with third parties and, therefore, did not suffer the injury that the VPPA was meant to protect" fails. Triller Mot. at 12.

As the legislative history makes clear, the VPPA was intended to prohibit, except in limited circumstances, the disclosure to public or private entities of records (or information derived from those records) kept by video tape service providers and linking users with the subject matter of the videotaped materials they have requested or obtained. S. Rep. No. 100-599, 100th Cong., 2nd Sess. 1988, U.S.C.C.A.N. 4342-1-4342-9, 1988 WL 243503. The clear intent of the VPPA is to prevent the disclosure of private information; as established by its legislative history, the VPPA enables consumers "to maintain control over personal information divulged and generated in exchange for

[11] It bears mentioning that simply because information has been associated with a "user id" or seemingly anonymized does not mean that it is anonymous at all. *See* Yarden Z. Kakon, *"Hello, My Name Is User #101": Defining Pii Under the Vppa*, 33 Berkeley Tech. L.J. 1251, 1256 (2018) ("Pseudonymization only acts as a superficial barrier to identification, as entities can re-identify a user by aggregating multiple datasets."); Suzanne L. Riopel, *The Price of Free Mobile Apps Under the Video Privacy Protection Act*, 6 Am. U. Bus. L. Rev. 115, 123-24 (2016) (noting that "[a] common misconception among consumers is that they remain anonymous by not registering or expressly disclosing personal information within a mobile app" because geolocation can identify them). The district court in *Yershov* also cautioned that "referring to these identifiers as 'anonymous identifiers'. . . is unhelpful and possibly misleading." *Yershov v. Gannet Satellite Info. Network, Inc*., 104 F. Supp. 3d 135, 146 (D. Mass. 2015), *rev'd on other grounds*, 820 F.3d 482 (1st Cir. 2016). For example, a Social Security number, standing alone, is anonymous, but "it would be absurd to conclude that a social security number is not PII." *Id.*

receiving services from video tape service providers." *Id*. This purpose is furthered by allowing plaintiffs to bring suit against app providers which share personal video viewing information in flagrant violation of the VPPA. *See* S. Rep. No. 100-599, 100th Cong., 2nd Sess. 1988, U.S.C.C.A.N. 4342-8, 1988 WL 243503 ("information collected for one purpose may not be used for a different purpose without the individual's consent").

Companies must provide "distinct and separate" disclosure, as required under the VPPA. Subsection (b)(2) of the VPPA authorizes disclosures to third parties only with the consumer's "informed, written consent" that is "distinct and separate" from any form setting out the consumer's "legal and financial obligations," and is either "given at the time disclosure is sought" or given in advance for a set period of time that cannot exceed two years. 18 U.S.C. § 2710(b)(2)(B). *See In re Hulu Privacy Litig.*, No. C 11-03764 LB, 2014 WL 2758598, at *18 (N.D. Cal. June 17, 2014) (holding that Facebook data policy did not qualify as VPPA consent); *In re Hulu Privacy Litig.*, 2014 WL 1724344, at *17 (same). Triller did not provide distinct and separate disclosure, nor did it allow for consumers to provide informed and written consent to the collection and sharing of PII. *See* Compl. ¶¶ 61-80.[12]

C. Plaintiff may seek injunctive relief against Triller for its failure to destroy improperly-collected PII.

While accurate that the VPPA does not authorize specific statutory damages related to Triller's failure to destroy information, in addition to statutory damages sought for Triller's other VPPA violations, Plaintiff seeks injunctive and declaratory relief against Triller related to its unlawful acts. *See* Compl. ¶ 90 (describing injunctive relief); 118 (seeking "other preliminary and

[12] Moreover, even if users did consent to Triller sharing information collected from users with third parties, the disclosures provided in Triller's Terms do not sufficiently inform consumers that Triller was sharing specific, video watch history. *Compare* Triller Mot. at 13.

equitable relief as the Court determines to be appropriate"). As noted by the court in *Sterk v. Redbox Automated Retail, LLC*, "absent the clearest command to the contrary from Congress, federal courts retain their equitable power to issue injunctions in suits over which they have jurisdiction." 672 F.3d 535, 539 (7th Cir. 2012) (quoting *Califano v. Yamasaki*, 442 U.S. 682, 705 (1979)). While Plaintiff is not pursuing damages for a violation of this section of the VPPA, she is seeking injunctive relief related to the destruction of PII that Triller improperly collected. Provided the Court has jurisdiction of this action, such a remedy is appropriate. *Sterk*, 672 F.3d at 539 (noting that express, statutory authorization is unnecessary for injunctive relief under the VPPA).

III. Triller violated the Illinois Consumer Fraud Act.

A. Plaintiff qualifies as a "consumer" under the ICFA; Triller's assertion that its app is "free" has no bearing on that determination.

Despite collecting and profiting from Plaintiff's use of Triller, Defendant argues that Plaintiff does not qualify as a "consumer" because she did not "make any purchase to use the Triller App." Triller Mot. at 19. But Triller fails to note that a plaintiff need not actually purchase "merchandise" with money in order to be a "consumer" under the ICFA. *See Liston v. King.com, Ltd.*, 254 F. Supp. 3d 989, 1006 (N.D. Ill. 2017) (holding that an exchange of marketing services for a good or service of value provided by the defendant allowed a plaintiff to meet the definition of "consumer" for ICFA purposes); *Bank One Milwaukee v. Sanchez,* 783 N.E.2d 217, 221 (Ill. App. 2003) (holding that the plaintiff asserting defendants forged her signature as a cosigner on a contract for the sale of a truck entitled her to relief under the ICFA).

When considering the ICFA, "courts should liberally construe and broadly apply the Act to eradicate all forms of deceptive and unfair business practices." *Kirkruff v. Wisegarver*, 697 N.E.2d 406 (1998). Here, as part of that liberal construction, Plaintiff also has standing to pursue a claim against Triller via the "consumer nexus test," which concerns "conduct [that] involves

trade practices addressed to the market generally or otherwise implicates consumer protection concerns." *Roppo v. Travelers Companies*, 100 F. Supp. 3d 636, 651 (N.D. Ill. 2015), *aff'd sub nom.* 869 F.3d 568 (7th Cir. 2017) (quoting *Downers Grove Volkswagen, Inc. v. Wigglesworth Imports, Inc.*, 546 N.E.2d 33, 41 (Ill. App. 2d Dist. 1989)).[13] To satisfy the "consumer nexus" test, a plaintiff must show "(1) that their actions were akin to a consumer's actions to establish a link between them and consumers; (2) how defendant's representations. . . concerned consumers other than [plaintiff]; (3) how defendant's particular [activity] involved consumer protection concerns; and (4) how the requested relief would serve the interests of consumers." *Roppo*, 100 F. Supp. 3d at 651.[14]

Plaintiff readily satisfies the test. First, she used a service offered by a commercial entity, and that commercial entity in exchange gathered and monetized her data without her consent. Compl. ¶¶ 38-60, 68. Next (satisfying the second, third, and fourth prongs of the test), Defendant's omissions, misrepresentations, and unfair business practices were not solely aimed at Plaintiff, but targeted all Triller app users; Plaintiff has alleged that Defendant is surreptitiously collecting and disclosing PII, which is a major consumer protection concern; and finally, if Plaintiff is successful in her claims, she will be successful not only on her own behalf, but on behalf of the absent class,

[13] "[T]here is nothing in the [ICFA] that suggests that it applies only to 'consumers[.]'" *Wiegel v. Stork Craft Mfg., Inc.*, 780 F.Supp.2d 691, 693-94 (N.D. Ill. 2011). *See also P.I.A. Michigan City, Inc. v. Nat'l Porges Radiator Corp.*, 789 F. Supp. 1421, 1427 (N.D. Ill. 1992) (denying defendant's motion to dismiss plaintiff's ICFA claims on the basis that plaintiff was not a consumer).

[14] The "consumer nexus" test is meant to protect individual persons who are like consumers, but have not actually purchased merchandise. *See GC2 Inc. v. Int'l Game Tech. PLC,* 255 F. Supp. 3d 812 (N.D. Ill. 2017) (holding that a plaintiff, developer of videos and images used on slot machines, properly alleged conduct akin to consumers under the consumer nexus test against a defendant licensee when the licensee fraudulently indicated that it owned the copyright to such images and videos, and plaintiff was sued for copyright infringement after downloading those images and videos for use, the same as other consumers were).

made up of Triller app users in Illinois. *See* Compl. at 31-32. As a result, even if this Court were to conclude that Plaintiff is not a "consumer" under the ICFA, Plaintiff (and the absent class) may still proceed under the consumer nexus test.[15]

B. The ICFA's extraterritoriality is irrelevant because the Plaintiff used the app in Illinois.

The ICFA allows a party to bring a private right of action for violations of the statute that occur in Illinois, which is what Plaintiff Wilson has alleged. Triller ignores the relevant case law interpreting the ICFA, and also fails to account for the most basic of pleading standards in federal court: that reasonable inferences must be drawn in favor of the non-movant.

While Triller is correct that the ICFA "does not have extraterritorial effect" and instead is limited to transactions that occur within Illinois, *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 853 (Ill. 2005), the Illinois Supreme Court has also acknowledged that the "situs of a consumer transaction" where "the transaction is made up of components that occur in more than one state" is not as simply determined. *Id.* (citing *Goshen v. Mutual Life Insurance Co.*, 774 N.E.2d 1190 (N.Y. Ct. App. 2002)). Illinois courts should consider "(1) the claimant's residence; (2) the defendant's place of business; (3) the location of the relevant item that is the subject of the disputed transaction; (4) the location of the claimant's contacts with the defendant; (5) where the contracts

[15] Even if Plaintiff does not qualify as a "consumer" under the Act, and the Complaint does not satisfy the "consumer nexus" test, Plaintiff is still entitled to relief under the Act. Section 10(a) of the ICFA provides, in part, that "[a]ny person who suffers actual damage as a result of a violation of [the] Act" may bring a cause of action against that person for consumer fraud. 815 ILCS 505/10a(a). *See also Thrasher-Lyon v. Illinois Farmers Ins. Co.,* 861 F. Supp. 2d 898, 911 (N.D. Ill. 2012) (holding that the ICFA does not appear to limit the private right of action to "consumers"); *Oliveira v. Amoco Oil Co.*, 776 N.E.2d 151, 155 (Ill. 2002) (expressly holding that Section 10a(a) "authorizes private causes of action for deceptive business practices proscribed by the Act" by "[a]ny person who suffers actual damage as a result of a violation of [the] Act committed by any other person."). Plaintiff has alleged that she and other consumers did sustain actual injuries as a result of Triller's unlawful conduct. *See, e.g.,* Compl. ¶ 90.h.

at issue were executed; (6) the contract's choice of law provisions, if there are any; (7) where the allegedly deceptive statements were made; (8) where payments for services were to be sent; and (9) where complaints about the goods or services were to be directed." *See The Clearing Corp. v. Fin. and Energy Exch. Ltd.,* No. 09 C 5383, 2010 WL 2836717, *6 (N.D. Ill. July 16, 2010) (citing *Avery,* 835 N.E.2d at 854-855)).

Applying this analysis to the present case, the Court should not automatically dismiss Plaintiff's claim. While the Defendant is headquartered in New York, the Plaintiff resides in Illinois and it is for this Court to draw the inference that she used the Triller app while in her home state,[16] where Triller collected her information without her consent. *See* Compl. ¶¶ 4, 7, 37-50. Especially where the statutory language provides that the ICFA should be construed to provide the broadest protection possible, the Court may apply this cause of action to Plaintiff's claim.

C. Plaintiff pleads a cognizable claim under the ICFA.

Plaintiff pleads a cognizable claim that Triller violated the ICFA, because Plaintiff has alleged sufficient factual support for the Court to infer that Defendant's "deceptive, unfair, and unlawful trade acts or practices" in violation of the Act caused her injuries. Plaintiff has complied with Rule 9(b) in alleging the "who, what, when, where, and how" of the alleged fraudulent misrepresentations and omissions. However, even if this Court concludes that Plaintiff's claims have not been pleaded with sufficient particularity as required under Rule 9(b), Plaintiff has pleaded sufficient facts under Rule 8 for her "unfair" claims, which is all that is required to state a claim for a violation of the Act by unfair business practices.[17]

[16] If the allegations are insufficient, Plaintiff may amend to add such details.

[17] In her Complaint, Plaintiff alleges that Triller misrepresented its data collection and distribution policies by not informing users of the app sufficiently that such data would be collected and/or distributed. In doing so, Plaintiff alleges the who: Defendant Triller discloses private information

Even if this Court were to determine that Plaintiff has not alleged fraud under the ICFA with sufficient particularity, this is not the end of the inquiry. Plaintiff has alleged facts to support that Defendant used "deceptive, *unfair*, and unlawful trade acts or practices" in her Complaint. Compl. ¶ 130 (emphasis added). Plaintiff need not satisfy Rule 9(b) to state a claim under the ICFA for unfair business practices "[b]ecause neither fraud nor mistake is an element of unfair conduct under Illinois' Consumer Fraud Act." *Windy City Metal Fabricators & Supply, Inc. v. CIT Technology Financing Services, Inc.*, 536 F.3d 663, 670 (7th Cir. 2008). Therefore, "a cause of action for unfair practices under the Consumer Fraud Act need only meet the notice pleading standard of Rule 8(a), not the particularity requirement in Rule 9(b)." *Id.* (citing *Tamayo v. Blagojevich*, 526 F.3d 1074 (7th Cir. 2008); and *Bell Atl. Corp. v. Twombly,* 127 S. Ct. 1955, 1964 (2007)). As a result, "under federal notice pleading standards, the complaint need only provide a short and plain statement of the claim that shows, through its allegations, that recovery is plausible rather than merely speculative." Fed. R. Civ. P. 8(a). Plaintiff has satisfied this standard.

---

to Facebook and Appsflyer, but does not state that that information will contain PII, and makes agreement to the Triller App's Terms and Conditions neither a prerequisite nor a condition of use of the Triller app. Compl. ¶¶ 38, 31-33. Plaintiff alleges the "what": Defendant discloses unique identifiers, sufficient to identify individual users of the app , to third parties without disclosing to the user that Triller will do so. *Id*. ¶¶ 42-54. Plaintiff alleges the where: Triller aggregates the data through its app , and transfers it from Plaintiff's phone in coded messages to third parties, including Facebook and Appsflyer, but does not include this information in its Terms and Conditions. *Id.* ¶¶ 42-54, 31-33. Finally, Plaintiff alleges the how: Triller makes its Terms and Conditions and Privacy Policy difficult to find, and does not require agreement of any kind to either set of terms prior to the collection and distribution it conducts. *Id.* ¶¶ 38, 31-33. Plaintiff alleges that the terms and conditions of the Triller app do not adequately define "personal information", and do not indicate whether "personal information" includes facial biometric identifiers, unique identifiers, or information that can, when aggregated or combined, be used to identify an individual. *Id.* ¶¶ 70-82. Such allegations express sufficient particularity, with regard to the named Plaintiff Ms. Wilson, as to what omissions and what misrepresentations were made to her, when and where, and how they were fraudulent.

Defendant finally argues that the Plaintiff has alleged no pecuniary loss. However, Plaintiff has alleged that her personal information and private data was collected and distributed to third parties without her knowledge or consent. Plaintiff's data has value. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 600-01 (9th Cir. 2020), *cert. denied sub nom. Facebook, Inc. v. Davis,* 141 S. Ct. 1684 (2021) (holding that because California law recognizes a legal interest in unjustly earned profits, Plaintiffs adequately pleaded an entitlement to Facebook's profits from users' personal data, and that such data had real value, because Facebook profited from this data). Just as in *Facebook*, where the Plaintiffs alleged that the defendant acquired users' sensitive and valuable personal information and sold it for a profit, so Plaintiff here has alleged that Defendant has been unjustly enriched by its distribution and sale of her valuable personal information without obtaining her consent. Plaintiff has both an interest in her own private, personal data, and an interest in any profits generated from that data without her consent. As a result, Plaintiff has sufficiently alleged "actual damages" in the form of pecuniary loss.

IV. Triller exceeded authorized access to Plaintiff's device, making this case actionable under the Computer Fraud and Abuse Act.

Plaintiff properly states a claim for violation of the CFAA because, contrary to Triller's assertions, the CFAA applies to Defendant's conduct as alleged in the Complaint. The plain text of the CFAA, as well as case law, supports the applicability of the CFAA to civil actions such as this and the statute on its face is not limited solely to "hacker-type" scenarios as Defendant contends. The facts here are even more nefarious—instead of an individual hacking into Plaintiff's phone, a company did so under the guise of providing a "free" app that stole and shared Plaintiff's sensitive information. Plaintiff's complaint properly states a civil claim for violation of the CFAA by adequately pleading that Triller exceeded authorized access to Plaintiff's device; and Triller's conduct resulted in economic loss greater than $5,000.

A. The CFAA applies in cases like this one.

The CFAA applies to Defendant's unauthorized collection of Plaintiff's personal information when Plaintiff downloaded and installed the app on her mobile device without being adequately informed that the app was collecting and sharing her sensitive personal information. While Defendant claims the CFAA is limited to "traditional" computer hacking schemes, the CFAA is not so narrowly construed. The text of the statute outlines its applicability to "whoever. . . knowingly and with intent to defraud, accesses a protected computer without authorization, or *exceeds authorized access*, and by means of such conduct furthers the intended fraud and obtains anything of value . . . ." 18 U.S.C. § 1030(a)(4) (emphasis added). The CFAA explicitly addresses when civil liability attaches, specifying damages are obtainable "if the offense caused. . . loss to 1 or more persons during any 1-year period. . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). Courts in this District and Circuit have also read the applicability of the CFAA to extend beyond traditional computer hacking. *See, e.g., Starwood Hotels & Resorts Worldwide, Inc. v. Hilton Hotels Corp.*, No. 09 CIV. 3862 (SCR), 2010 WL 11591050, at *4 (S.D.N.Y. June 16, 2010) ("Although Defendants attempt to limit the reach of the CFAA, arguing that the CFAA is intended to address only computer hacking, other courts have given the CFAA a far broader scope. Under this broader view, the statute may encompass limits placed on the use of information obtained by permitted access to a computer system.").

To support its argument that the CFAA is inapplicable, Defendant relies primarily on one distinguishable California district court case, *Welenco, Inc. v. Corbell*, by mischaracterizing its facts and conclusions. *See* Triller Mot. at 6. First, *Welenco* concerned a geo-logging company where the complaint alleged that a former employee had formed his own, competing entity by using confidential business information obtained while still employed at Welenco. 126 F. Supp.

3d 1154, 1161 (E.D. Cal. 2015). Second, the court in *Welenco* was ruling on a summary judgment motion, based on a full discovery record. *Id.* at 1161-62. Finally, the *Welenco* court acknowledged the applicability of the CFAA to the broad range of civil cases, although Defendant claims it does not: "While the statute is criminal in nature, civil liability may attach if the loss is greater than $5,000. 18 U.S.C. § 1030(c)(4)(A)(i)(I)." *Id.* at 1168.[18]

Courts have routinely applied the CFAA in civil cases like this one. For example, in *Bowen v. Porsche Cars, N.A., Inc.*, No. 1:21-CV-471-MHC, 2021 WL 4726586 (N.D. Ga. Sept. 20, 2021), the court denied a motion to dismiss despite defendant's arguments that the purchase of a vehicle with an antenna that received satellite radio transmissions amounted to consent to receive the software updates that modified the vehicle. *Id*. at *4. There, a class of plaintiffs alleged a violation of the CFAA when defendant sent a software update that caused plaintiffs' vehicles' system ("PCM") to malfunction. The court reasoned that "Bowen's tacit consent to receive satellite radio signals does not imply consent to modify his vehicle's software. . . . While the satellite antenna may utilize the PCM, nothing in the facts alleged implies that access to the antenna or consent to receive satellite radio transmissions is the same as an authorization to directly access, much less modify, the PCM." *Id*. Just because a company such as Triller may have had consent to install an app on a consumer's phone, it does not justify the collection and dissemination of security-sensitive and private information concerning the Plaintiff.

[18] In *University Sports Publications Co. v. Playmakers Media Co.*, another case that Triller cites, the court determined that an administrator had not exceeded his *authorized access*; accordingly, there was no CFAA violation. 725 F. Supp. 2d 378, 384-85 (S.D.N.Y. 2010). *See also Cenveo, Inc. v. Rao*, 659 F. Supp. 2d 312, 316 (D. Conn. 2009). Plaintiff explicitly argues that Triller *did* exceed its "authorized access" to her device through the collection *and* dissemination of information to which she did not consent nor know that Triller was collecting.

1. Triller exceeded authorized access and caused economic loss.

Triller asserts Plaintiff has failed to sufficiently allege that it exceeded its authorized access to Plaintiff's device. Triller Mot. at 7. This is incorrect.

The phrase "exceeds authorized access" in the context of the CFAA is not merely limited to cases in which a person accesses confidential information stored on the physical device. *See, e.g., Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F. Supp. 3d 1056, 1070 (N.D. Cal. 2018). In *Synopsys*, the defendant sought dismissal asserting that the plaintiff failed to plead impermissible access to computers in its CFAA claim. The court disagreed, finding the facts of the case "fit [] within the 'exceeds authorization' line of cases. . . *based on the hidden presence of software that accesses, obtains, and transmits information that a party was not entitled to access, obtain, or transmit.*" *Id*. (emphasis added, citing *Flextronics International, Ltd. v. Parametric Technology Corporation*, 2014 WL 2213910, at *3 (N.D. Cal, May 28, 2014). In *Feldman v. Comp Trading, LLC,* the court denied defendant's motion to dismiss plaintiffs' claim under the CFAA despite defendant's argument that plaintiffs were investigating a breach of a cloud-based server rather than the computer, itself. *Feldman v. Comp Trading, LLC*, No. 19CV4452, 2021 WL 930222, at *6 (E.D.N.Y. Mar. 11, 2021). Here, Plaintiff similarly alleges Defendant's conduct exceeded any authorized access given Triller's lack of disclosure or consent to its software collecting, storing, and sharing PII. Compl. ¶ 100.

Similarly, "economic loss" under the CFAA is not measured solely in terms of the cost to restore data to the condition in which it existed prior to a violation, as Defendant claims. Triller Mot. at 8. Numerous cases found that data need not be physically changed or erased for there to be damage under the statute. *See Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 894-95 (N.D. Cal. 2010) (citing *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.,* 119 F.

Supp. 2d 1121, 1126-27 (W.D. Wash. 2000), *Therapeutic Research Faculty v. NBTY, Inc.,* 488 F.Supp.2d 991, 996 (E.D. Cal. 2007)).

Further, "loss" under the CFAA is broadly defined as "any reasonable cost to any victim," including actions such as "the cost of responding to an offense, conducting a damage assessment, and restoring the data. . .and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 934 (9th Cir. 2004) (quoting 18 U.S.C. § 1030(e)(8)).

In *SuccessFactors Inc. v. Softscape, Inc.*, the court held:

> [W]here the offender has actually accessed protected information, discovering who has that information and what information he or she has is essential to remedying the harm. In such cases courts have considered *the cost of discovering the identity of the offender or the method by which the offender accessed the protected information to be part of the loss for purposes of the CFAA*.

544 F. Supp. 2d 975, 981 (N.D. Cal. 2008) (emphasis added). In *Starwood Hotels & Resorts Worldwide, Inc. v. Hilton Hotels Corp*., the court denied defendant's motion to dismiss, finding plaintiff sufficiently alleged "loss" under the CFAA in the form of ongoing efforts to determine what confidential material was taken from the plaintiff's computer systems. No. 09 CIV. 3862 (SCR), 2010 WL 11591050, at *7 (S.D.N.Y. June 16, 2010). The court reasoned: "the full extent of how the information may have been used by Hilton and the individual defendants is not yet fully known, but will become fully known through the discovery in this action. . . . The Court concludes that these factual allegations are sufficient to state a claim for loss that is facially plausible and that Starwood 'is entitled to offer evidence to support the claims.'" *Id.* (citing *York v. Association of the Bar of City of New York*, 286 F.3d 122, 125 (2d. Cir. 2002)). *See also ML Fashion, LCC v. Nobelle GW, LLC*, No. 21-CV-00499 (JCH), 2022 WL 313965, at *19 (D. Conn. Feb. 2, 2022) (denying defendants' motion to dismiss plaintiffs' CFAA claim, finding plaintiffs adequately

alleged a claim under the statute by pleading loss in the form of "investigating the theft and misuse of. . . computers.").

Here, Plaintiff's "loss," which include threats to public safety given the numerous privacy violations (Compl. ¶ 101), can be measured in terms of the cost of discovering and identifying the PII accessed, collected, and disseminated without Plaintiff's consent Compl. ¶ 101. Additionally, Plaintiff's loss concerns intangible property, including confidential data, which can constitute a thing of value. *See United States v. Ivanov*, 175 F. Supp. 2d 367, 371 (D. Conn. 2001) (noting that confidential data constitutes property). *See also Carpenter v. United States*, 484 U.S. 19, 25 (1987) (noting that the "intangible nature [of confidential business information] does not make it any less 'property' protected by the mail and wire fraud statutes.").

CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court deny Triller's motion to dismiss.

Dated: March 14, 2021

Respectfully submitted,

/s/ Amy E. Keller

Adam J. Levitt
Amy E. Keller (*pro hac vice*)
James Ulwick (*pro hac vice*)
DiCELLO LEVITT GUTZLER LLC
Ten North Dearborn Street, Sixth Floor
Chicago, Illinois 60602
Tel.: (312) 214-7900
alevitt@dicellolevitt.com
akeller@dicellolevitt.com
julwick@dicellolevitt.com

David A. Straite
DiCELLO LEVITT GUTZLER LLC
One Grand Central Place
60 East 42nd Street, Suite 2400
New York, New York 10165
Tel.: (646) 933-1000
dstraite@dicellolevitt.com

Lesley E. Weaver (*pro hac vice*)
Anne K. Davis (*pro hac vice*)
Joshua D. Samra (*pro hac vice*)
BLEICHMAR FONTI & AULD LLP
555 12th Street, Suite 1600
Oakland, California 94607
Tel.: (415) 445-4003
lweaver@bfalaw.com
adavis@bfalaw.com
jsamra@bfalaw.com

Javier Bleichmar
BLEICHMAR FONTI & AULD LLP
7 Times Square, 27th Floor
New York, New York 10036
Tel.: (212) 789-1340
jbleichmar@bfalaw.com

James J. Pizzirusso (*pro hac vice*)
HAUSFELD LLP
888 16th Street, NW, Suite 300
Washington, D.C. 20006
Tel.: (202) 540-7200
jpizzirusso@hausfeld.com

Steven M. Nathan
HAUSFELD LLP
33 Whitehall St., 14th Floor
New York, New York 10004
Tel: (646) 357-1100
snathan@hausfeld.com

Counsel for Plaintiff and the Proposed Class and Subclasses

CERTIFICATE OF FILING

I hereby certify that a copy of the foregoing was filed using this Court's CM/ECF service, which will send notification of such filing to all counsel of record this 14th day of March 2022.

/s/ Amy E. Keller
Amy E. Keller